Vendor Risk Management
Overview

• Security and Risk Landscape
• Mechanics of a Program
• Common Approaches (Mistakes)
• Uncommon Ground (Suggestions for the Future)
• Addressing Specific Questions and Concerns
Bet you didn’t know

• Background checks are conducted in the city and states where you have lived and worked. ONLY.
• BYOD + DLP = 0
• No one gets asset management right
• Same for configuration management
Case Study Slide

Epilson

Name and Email address

Spear Fishing

Target

HVAC

Spear Fishing (Citadel)
Mechanics of a Program

- New Vendor Onboarding
- Inventory of vendors and contact information
  - Contract status and rights
- Methodology to assess risks
  - More on this later

- Vendor outreach, questionnaires / procedures
- Follow-up on issues
Enterprise Grade Options

**Termination / Off-boarding**
- Data rights, obligations
- Consider backup tapes, intellectual property and email

**Analysis and Reporting**
- Which vendors are riskiest? XYZ Corp?
- Which areas are riskiest across all vendors? BYOD? Malware protection?

**Communication**
- Discuss the results with key stakeholders?
- Inform the vendor where they stand compared to others?

**Vendor Standards**
- Do RFP’s, and contracts include stated requirements?
- Are the standards realistic? Appropriate?
Risk Assessment

• Triage
  – Developing a method to initially assess the level of risk at each vendor

• Risk Response
  – Questionnaires
  – 3rd Party Assurance
  – Onsite Interviews
  – Onsite procedures
  – Frequency of follow-up

• Analysis of Results
  – How did the risks at this vendor differ from others?
  – What are typical practices in the industry?
From the Trenches

• N/A is never a good idea
• Long questionnaires just don’t work
• Building relationships can help, but what is your capacity to manage those relationships?
• If you could address just one risk, what would it be?
• A SOC 1 is suitable for ICFR only
Following Up

- Realistically assign or agree to deadlines
- Automation is key here
- Understand the root cause (if and when possible)
- Be sure remediation plans are specific, time based and measurable
  - Compare commitments to develop “a policy” vs. adopt specific policy requirements
  - Focus on self-corrective measures
## Measuring Program Effectiveness

### Focus on observable data vs. risks
- Trend of sensitive data records encrypted at rest
- Trends related to the number of vendors that `<insert risk metric here>`

### Coverage
- Metrics that relate to investment (cost) to items such as
  - # key vendors addressed
  - depth of coverage
  - Value to services rendered by the vendors (individually and in aggregate)
### More from the Trenches

| “Yes, I review that periodically” | • Really?  
| | • What period? When was the last review? What did your last review uncover? What initiated that review? |
| “No, sensitive data is NEVER handled via email” | • Really?  
| | • Are client matters ever discussed among managers via email? What communication method is utilized when primary systems are down? |
| “We’re planning that for next year” | • Really?  
| | • Can I see your project plan? What is the status of budget allocated for those activities? |
Cloud Considerations

• Everyone is at AWS, but did you know I can rent space on the same hardware as my target?

• Some cloud vendors allow tenants to encrypt data in a manner that “locks out” the cloud service provider (Kudo’s to ServiceNow)

• It will not be possible to conduct a detailed forensic investigation at a major cloud services provider (ever at SaaS and PaaS, almost never at IaaS)
Wave Your Magic Wand

• Two Factor Authentication
• Internal processes for secure software development
• Encryption at rest
• Meaningful security monitoring